Children’s Privacy and the Justification of ICT-based Parental Monitoring

Zhihao Lin

Supervisor: Elin Palm
Examiner: Lars Lindblom
Abstract:

As Information and Communication technology (ICT) has rapidly advanced in China, parental monitoring may invasively penetrate into children’s privacy, while China is lagging behind on the issue of children privacy protection. Privacy is invaluable to human development, and children do have interests in their privacy. This thesis is going to investigate under which condition it is desirable for parents to apply ICT techniques to monitor children, which does not invade children’s privacy. Before reaching the decision of carrying out monitoring, the intent and the necessity of monitoring should be considered. Children should be informed and their consent should be acquired before deploying monitoring. After the decision is made, the proportionality of monitoring practice requires parents to opt for the least invasive and the most necessary approach. Besides parental monitoring, states and schools can offer media literacy education to enable children to protect themselves from privacy infringement.
Acknowledgement

Throughout the writing of this thesis I have received a great deal of support and assistance. I would first like to thank my supervisor, Prof. Elin Palm, whose expertise was invaluable in the formulating of the research topic and methodology in particular. Her patience, motivation, and immense knowledge helped me in all the time of research and writing of this thesis.

I would also like to express my gratitude to my friends, Ms. Yingqi Luo, Ms. Peishan Tan, Mr. Di Cui and Mr. Kun Qian, for their genuine support and encouragement. In addition, I would like to thank my classmates from the programme, who are really supportive and kind to me.

Last but not the least, my acknowledgement would be incomplete without thanking my family, especially my mother Mrs. Wenhua Lin and my father Mr. Xiting Lin. They have always been caring and supportive. Their encouragement helped me get through the tough moments when I was writing the thesis.

Linköping in May 2019

Zhihao Lin
Table of Contents

CHAPTER 1: INTRODUCTION ....................................................................................... 1

CHAPTER 2 THE CONCEPT OF PRIVACY AND EMERGENCE OF THE ISSUE OF CHILDREN’S PRIVACY .................................................................................................................. 4

  2.1 INDIVIDUAL ICT PRIVACY AND CHILDREN’S INVOLVEMENT IN ICT IN CHINA .......... 5
  2.2 BRIEF INTRODUCTION OF PRIVACY ........................................................................ 9
  2.3 CHILDREN’S PRIVACY ............................................................................................ 13

CHAPTER 3 JUSTIFICATION OF ICT-BASED PARENTAL MONITORING AND MEDIA LITERACY EDUCATION ........................................................................................................ 20

  3.1 MACNISH’S THEORY AND JUSTIFYING ICT-BASED PARENTAL MONITORING .......... 20
  3.2 MEDIA LITERACY EDUCATION .................................................................................. 28

CHAPTER 4: CONCLUSION ....................................................................................... 30

REFERENCES ............................................................................................................. 32
Chapter 1: Introduction

During my stay in Sweden, the only way I could keep in touch with my family and friends in China is contacting them via Wechat, a messaging and social media app developed by Tencent. There is a section in Wechat named Moment allowing users to share videos and photos with their friends or followers. The majority of contents displayed in my Moment page are footages and pictures depicting new born babies or children reaching developmental milestones, which I find interesting and inspiring.

The joy of watching children’ funny moments starts disturbing me after I came across several articles describing issues brought by parents posting children’s pictures on social media without realizing risks and harms. Children and teenagers claim they felt horrified and unsettled when they googled their names and found images revealing their personal and school life. What frustrates them most is that their parents share these photos without their consent (LORENZ, 2019). Pictures and personal information forms one’s online identity which is likely to last for life and impossible to (1) be deleted or (2) be retrieved. A survey conducted in 2010 finds that at least 70% of toddlers under the age of 2 have their digital footprints created by their parents uploading images or creating social media accounts (AVG, 2010). Parents unconsciously reveal their children’ appearance, personal traits, schools and health history when sending posts on Facebook, Twitter or Instagram. These data could be exploited by hackers or child predators even the posts are only made available to close friends or family members. Digital devices such as smart speakers at home or sports watches for children could also send sensitive data like location to developers without users’ approval (Lieber, 2018).
Besides excessive sharing on social media and purchasing digital devices without paying attention to data agreement, employing GPS tracking technology on children also poses ethical problems. A study conducted in UK reveals that pupils state that being monitored by massive CCTV frustrates them as they perceive cameras installed within campus as a symbol of mistrust. Moreover, they complain that schools have infringed their privacy (Taylor, 2010). Given follow-up researches results and increasing awareness of children privacy, scholars (Fahlquist, 2015, Taylor, 2010) suggest that although GPS tracking technology is applied at school for the purpose of safeguarding children, the risk that ethical issues pertinent to children’s privacy must be recognized. When children become teenagers, their sense of privacy accordingly reaches a further level. Parents frequently justify their violation of teens’ privacy by claiming that their children do not value privacy as they post their pictures or comments on Facebook or Twitter. However, researchers point out that teenagers consider privacy important that they demand control over their information both online and offline. Teenagers sharing personal information on social network sites does not indicate that they devalue privacy. (Danah Boyd, 2017).

With advancing technologies and widespread social media, parents could extend their control over children’s privacy before adulthood, while in some extreme cases, taking care of handicapped or cognitively impaired children requires a 24/7 surveillance system through their entire life. ICT (Information and communications technology) (contributors, 2019b) based parenting, as an emerging form of parenting, is justified by keeping children from juvenile delinquency. Social sciences and psychology scholars, Margaret Herr and Håkan Stattin (Stattin and Kerr, 2000) challenge this notion by arguing that parenting quality should not simply rely on parental surveillance, but parents should positively engage children in daily conversations,
which encourage children to voluntarily share their latest information. Apart from parental monitoring, parents sharing children’s digital profiles, such as birthday pictures, school videos, raises concerns that these contexts contains sensitive personal data which could be exploited by hackers or make children vulnerable to cyber violence (Steinberg, 2016).

Bringing up a child is a demanding job requiring various levels of parental involvement. It is understandable that parents tend to shield their children from activities which could hazard their physical and mental wellbeing. By accessing children online footprints with technical methods, parents manage to keep a close eye on their children, but a question should be asked is that to what extend could this form of involvement be seen as justified.

This article intends to investigate the issue that under which conditions it is desirable for parents to apply ICT techniques to monitor children, which does not invade children’s privacy. Some may question that privacy is a western societal construct, which is not a universal value without the same meaning and–importance in Asian countries. This critique ignores the determined efforts Asian countries recently made to protect individual privacy. Generally, Universal Declaration of Human Rights states that people have a right to privacy and should be free from arbitrary interference (UN, 10 December 1948). Forty eight countries then voted in favor of this UN declaration, including China (UN, 1949). Some southeast Asian countries, like Japan (JAPAN, 2005), South Korea (KOREA, 2012), Singapore (SINGAPORE, 2012), Malaysia(MALAYSIA, 2010) and Vietnam(VIETNAM, 2016) have introduced laws to offer protection against privacy infringement. The improvement in legal work demonstrates that privacy is an indispensable value shared by Asian societies.

To fulfill the aim of this article, four chapters are devoted to answer the research question.
Chapter 1 servers as an introduction, providing readers with an overview of the research background and presenting the structure of this article. Chapter 2 starts with a summary of children’s involvement in ICT in China, while how Chinese government and the tech industry protect children’ privacy would be introduced as well. The analysis of Chinese cases would present the necessity of discussing the issue raised by this article. The second part of Chapter 2 is going to discuss these questions: 1) What is the meaning and value of privacy and what is privacy in relation to children; 2) Why children’s privacy should be given particular consideration; 3) If children’s privacy is of great value, to what extent should children be given rights to their own privacy and under what conditions should parents safeguard children’s privacy?

Since parts of parenting involve protecting children from various harms, including those from ICT, traditional parenting models overlap issues of children privacy. Therefore, Chapter 3 focuses on the normative analysis, adopting Macnish’s theory, which draws on the framework of the just war tradition (Macnish, 2014), in the hope of exploring the justification of parental involvement. This part also suggest that parents and states offer media literacy education to serve children’s best interests in terms of privacy.

Chapter 4 serves as the conclusion of this thesis.

Chapter 2 The concept of privacy and emergence of the issue of children’s privacy

This chapter will summarize children’s involvement in ICT in China as well as compare
China’s laws and regulations relevant to individual privacy, particularly children’s privacy, to its western counterparts. Then, it will examine several essential issues related to children’s privacy, which lays the foundation for further analysis in Chapter 3.

2.1 Individual ICT privacy and children’s involvement in ICT in China

A 2018 survey, conducted by China Internet Network Information Center (CNNIC), reveals that the total number of Internet users in China reached 802 million. 98.2% of surveyed users access Internet via cell phone. On average, a China netizen spends 27.7 hours surfing the Internet on a weekly basis. People aged 10-19 account for 17.5% of the overall sample, while they are the major users of mobile phone applications as well (CNNIC, 2018). Compared with the Internet penetration rate\(^1\) in China, which is 59.6%, the rates in the US and the European Union are respectively 88.1% (Stats, 2018) and 90.5% (Stats, 2019).

CNNIC partnered with Communist Youth League of China to carry out another research (CNNIC, 2019), detailing children’s online activities. The findings demonstrate that 92% of the research participants access the Internet via mobile phone. Regarding online activities, online learning accounts for 87.4%, which is followed by gaming, music consumption and messaging. Less than a quarter of the participants report addiction to Internet. Nearly 16% of minor users claim they suffered cyber bullying. The research team offered five suggestions to the government, the tech industry and caregivers, none of which mentioned children privacy protection. As for the US and the European Union, the children Internet usage rate in the US in

---

\(^1\) The Internet Penetration Rate is referred as the percentage of a population in a given country or region that uses the Internet. See https://www.igi-global.com/dictionary/internet-penetration-rate/15439
2015 is 71% of children aged 3 to 18 accessing the Internet (NCES, 2018), while in 2016 91% of young people in the EU were netizens (Eurostat, 2017).

Along with the enlarging Internet usage, countries, particularly those with advanced technological development, around the globe have increasingly placed high value in personal data protection, but China has lagged behind on this issue, while the scale of state surveillance over citizens is dramatically expanding.

Individual privacy protection is not adequately protected, partially due to lack of clear definition of privacy in China legal system (Yao-Huai, 2005, Banisar, 1999-2000). An international report points out that since 1999, Chinese government has installed Internet Great firewalls to block any attempt to access foreign websites, while at that time no law was introduced to offer general data protection (Banisar, 1999-2000). At the beginning of 2017, all telecom services providers, like China Mobile and China Union, were required to register every user’s identification (Yunjing, 2017). Back in 2010, only those who intended to buy a new sim-card, had to present their identification cards (Yannan, 2010). Personally, I registered my personal information earlier than 2017, when I got a message informing me that failure to get verified would result in terminating phone service. More invasively, Cyberspace Administration of China (“CAC”) in 2017 issued the Provisions on the Administration of Internet Comments Posting Services, which has been effective and requires all Internet platforms shall not allow any comments posted by users who failed to provide ID information. The official states the purpose of the provisions is to combat anti-government contents and promote a healthy cyber market (CAC, 2017a). Tech companies revise their policies to comply with the tightened regulations. Take Wechat, an messaging app used by 1.1 billion people
(Tencent, 2018), as an example, according to its latest policy, to create a new account later, a user has to offer a validated mobile phone number, which is attached to an ID number in the case of a Chinese citizen (ChinaHelp, 2018).

Children in China are not only subjected to online monitoring, but their physical daily lives are also permeated by ascending level of surveillance. Some schools reportedly require students to put on chip-equipped uniforms to track their location (Gartenberg, 2018), or employ facial recognition technique to capture and analyze students’ emotional activities during class (Chan, 2018). As for parents, smart watches marketed for children are trending in China, which track children’s real-time location and allow them to make phone calls to parents (Service, 2018). The privacy concern is rarely mentioned in China’s growing market, while in the EU, several products were ordered to be forcibly recalled due to violation of children privacy (Cimpanu, 2019) and a Norwegian consumer report uncovered sever security flaws in smartwatches (NCC, 2017, Lomas, 2017).

Compared with its radically expanding Internet usage and escalating scale of invasive surveillance, China’s legal action to combat personal data infringement is progressing, but there is still a large room for improvement, especially on the issue of children privacy. The first basic law to offer personal information protection on a state level is China Internet Security Law, also referred as Cyber Security Law of the People’s Republic of China, enacted in November, 2016. All tech or Internet companies running business in the file of data or network services in China are subjected to this law, which requires operators to guarantee users’ data security (Standing Committee of the National People's Congress, 2017). To further clarify individual data protection regulations, Chinese authorities in 2018 issued Personal information security
specification, which shares the principle of Cyber Security Law and draws on GENERAL DATA PROTECTION REGULATION (GDPR) in the EU. This specification offers detailed account for personal data collection, processing, sharing and disclosure (SAC, 2018). Obtaining users’ express consent is placed significant emphasis throughout the overall provisions (Hong, 2018, Lai, 2018). Besides Cyber Security Law and the latest specification, parents and the academia call on the Chinese authorities to tighten up laws to create a harmless online environment for minors. The bill was first introduced in 2016 and open to public discourse in 2017, but has not been enacted yet, which implies there is no effective law specifically address the issue of children ICT privacy (CAC, 2017b). The majority of the bill focuses on filtering online content and preventing addiction to Internet. Only article 16, 17 and 18 touch on the point of children data collection and consent acquisition (CAC, 2016), while these articles fail to offer constructive guidelines to minor users and their caregivers as well as miss the issue of parental control over children’s online footprints.

As for developed countries and international organizations that stick to the value of individual privacy, legislation shielding children from online privacy infringement has been brought in and revised frequently. In 2018, UNICEF issued a guideline, CHILDREN’S ONLINE PRIVACY AND FREEDOM OF EXPRESSION, to offer general principles and practical suggestions to information and technology industry to deal with issues relevant to children privacy. As this document states, children should be granted the right to their privacy and data (UNICEF, 2018). In the US, Children's Online Privacy Protection Act has come into effect since 2000. This law requires web operators and online service providers to seek parental consent before collecting underage users’ information. A failure to comply with the law could
lead to stiff punishment, including fines (contributors, 2019a). Similarly, in European Continent, article 8 of GDPR stresses that data of a child under 16 shall not be processed unless parents provide their authorization (Union, 2016). After the introduction of GDPR, some experts and scholars are concerned that a teen’s free access to abundant educational information and activities could be deprived, if he fails to get parental consent (TURK, 2018). Parents’ roles, as the above laws state, are children’s guardians combating exploitation from online corporations, but what if parents abuse their power under the guise of security or fail to assume responsibilities?

Since China has seen radical Internet and technology development, the rising public awareness of individual privacy urges the China authorities to strengthen its legislation. Personal data protection laws in developed countries serve as an example worth drawing on to China, but a common issue appears in different states’ regulations is the overrated role of parents and the undervalued recognition of a child’s control over his ICT privacy. Before addressing this issue, questions need to be answered are that what privacy is and why privacy is of importance to a child.

2.2 Brief introduction of privacy

Privacy is an elusive issue frequently discussed by scholars and the public. The scope of privacy has changed from time to time and no conclusive definition has come into existence. More importantly, a general feature of the most influential privacy accounts however, is that they focus adult subjects, quite often linking privacy to rational agency and autonomy. This article intends to underscore the value of privacy, particularly to children. First general value
of privacy will be covered ahead. Then, the discussion will be specifically directed to children’s perception of privacy ways in which privacy infringements may affect children.

The history of privacy could be traced back Aristotle’s contribution to separate political involvement and family lives (DeCew, 2018). A sophisticated account of privacy is provided in the article written by Samuel Warren and Louis Brandeis, in which they argue that the scope of the right to life has extended from tangible property to intangible possession, namely the right to be let alone. They warned for the invention of photography and unregulated journalism would expose personal life, inflicting mental and physical harm, eventually undermining one’s personality (Warren, 1890).

The value of privacy to form a human’s complete personality has gained popularity from philosophers around the globe. Charles Fried extends Warren and Brandeis’s argument to the sphere of interpersonal relationships, noting that keeping one’s information from unintended exposure allows oneself to establish intimate relationships, including love, friendship and family. The maintenance of intimacy eventually makes one’s basic needs met (DeCew, 2018).

Bruce Schneier, a cyber security expert, argues that, on a societal level, a significant implication of privacy is boosting development by encouraging experimentation. Controversial issues like same sex marriages or marijuana consumption, were immoral and illegal in the first place. It is those activists, who had privately strived to combat homophobia or test the acceptable amount of harmless usage of marijuana, making progress possible. If states had deprived their privacy by invasive monitoring and interference, none of these changes would have occurred (Schneier, 2016).

The notion that a right to privacy is valuable to personal development is gaining increasing
acceptance. As for what values of privacy laws should protect, the term, ‘control over one’s information’ is too ambiguous to determine what constitutes deprivation of one’s control. Countries’ differentiated conceptions of what constitutes privacy have led to disparities between regulations in various regions. Cambridge Dictionary refers privacy as someone’s right to keep their personal matters and relationships secret (Cambridge, 2019). In the US, Justice Stevens offers an explanation in a landmark case that constitution should protect two dimensions of privacy, which are controlling disclosure of personal information and reaching an individual decision free from government interference (Court, 1977, contributors, 2018). This account intertwines privacy with autonomy and free speech, which requires a government to restrict its interference. A 2013 research examined countries’ achievements or power abuse in the sphere of privacy around the world, based on the criteria of six conditions, such as effective privacy laws, free access to Internet, actively protected free speech. Spain claimed the first place, while Malaysia was ranked the worst country. The US and China were respectively criticized for massive surveillance programme and stringent Internet censorship (KELLY, 2013).

In a democratic society, the implications of privacy protection are to guarantee citizens own discretion over personal spaces, individual choices and particularly individual liberty (DeCew, 2018).

The value of privacy is not entirely determined by what is deemed private by an individual or what a state should safeguard, but also affected by social contexts and interpersonal relationships. Helen Nissenbaum argues that cultural integrity could serve as a compelling normative benchmark of privacy, which consists of two norms, norms of appropriateness and norms of distribution (Nissenbaum, 2004).
Norms of appropriateness state that how appropriate the information one intends to reveal depends on situations and on the particular of the ongoing conversations. Accordingly, what one perceives as sensitive should be left to be one’s privacy. For instance, one might share personal status, such as salary, medical history, finances with a life-long friend, but not with an acquaintance in workplace. A patient should inform his physician of his symptoms so he could receive effective treatments, while it is not necessary to share his retirement plan unless his physician requires him to do so (Nissenbaum, 2004).

While norms of appropriateness demonstrate the rationale for individual information disclosure, norms of distribution address issues related to the flow of information. The distribution norms draw on Michael Walzer’s theory, which notes that social justice should be achieved by distributing social resources based on different criteria. Similarly, whether the flow of information is allowed or prohibited should be determined by scenarios. Therefore, various context-based principles integrate into the distribution norms, such as confidentiality, need, free will. If an individual is notified by his friend that his personal life should not be disclosed to a third party, he should stick to the principle of confidentiality. Addresses and telephone numbers are necessarily passed from one post office to another to guarantee package delivery (Nissenbaum, 2004).

From the academic researches mentioned above, the generally acknowledged value of privacy to an individual is that one could accomplish his life plans or achieve a complete personality by exerting control over his personal information.

Nissenbaum’s argument sheds light on what information should remain in an individual’s territory unless he considers it appropriate and necessary to disclose. A child or a teenager
interprets virtual or physical context in a way different from adults. Research studying high school students’ information disclosure on Myspace found that underage users’ online behavior is driven by peer pressure, while the view of safety is inconsistent between parents and children. Parents were asked to classify information disclosure items as dangerous or safe, while children were asked to review and give feedback about the parents’ results. It turns out that on the privacy issue, children appear to be more relaxed than parents. The revealing findings are 1) the more a child values his own privacy, the less likely he could reveal himself online and 2) younger children are vulnerable and tend to disclose more information online. (De Souza and Dick, 2009).

The discussion of general value of privacy leads to the following subsection, which is going to answer what privacy is from a child’s angle, how being in possession of one’s privacy could positively affect a child’s development and what or whose interest is at stake when parents invasively surveil their children.

2.3 Children’s privacy

Children’s perception of privacy in relation to ICT would change as their cognitive and social developments advance. UNICEF refers a child as a human being under the age of eighteen (UNICEF, 1989). Minors younger than eighteen assume limited liabilities for their act in Chinese legal system (CHINA, 2007). To place children under one age group may ease law enforcement’s pressure, but this rough classification neglects the fact that an infant could hardly view privacy in the similar way as a teenager does, while both of them fit in the category of children. American Academy of Pediatrics (APA) notes that before entering adulthood, a child
would experience six developmental stages, ranging from Baby to Young adult. Each stage requires particular parental attention and public services, such as toilet training for toddlers, substance use consultation for teens (APA, 2019).

Since privacy partially refers to one’s control over his personal information, a precondition of claiming ownership of privacy is being able to distinguish oneself from others, which requires a sense of self. Self-consciousness advances as a child enters different developmental stages. The awareness of self emerges since toddlerhood (Josephine Ross, 2016). Afterwards, children’s advancing self-awareness allows them to participate in complicated social activities and establish interpersonal relationships. Remaining in solitary status occasionally allows young children to daydream and reflect on themselves, which is essential to their healthy development (Readdick, 1993). Teenagers attain a higher level of self-consciousness, which allows them to create abstract and sophisticated societal constructs, such as social status in peer groups, careers, achievements (Case, 1991). Variations in a sense of self lead to changes in a child’s perception of privacy. For instance, when a child starts to own a single room, his room is his territory. In his private space, he enjoys writing diaries and keeps them well hidden in his drawer. As he approaches puberty, he craves frequent interactions with his peers and adventures outside home or school. For the first time, the child creates social media accounts, which is only accessible to his followers. Regardless of age, a child would feel irritated, frustrated and mistrusted if his parent accesses his physical or virtual territory without permission.

Extensive parental interference may breach children’s privacy, resulting in deprivation of their chances of exploring. It is a parent’s primary responsibility to safeguard their children against potential harms. Some parents may install parental control softwares on their children’s
computers or smartphones to check their children’s browsing history or limit their screen time. Parents expect these apps could save minor users from the evil of Internet world and present them with a flawless utopia. Parents also fear children will become addicted to online games or social media or exposed to explicit context, which makes time limit and context filter most desirable functions of control apps (Hill, 2019). Kay Mathiesen, an information researcher, criticizes the practice of online monitoring and argues that parental monitoring impedes children developing full autonomy as well as poses threat to familial intimacy. Mathiesen notes that children deserve privacy in accordance to their level of autonomy, so they can be in control of online information exchange, which is fundamental to personal identity (Mathiesen, 2013). As for children’s perception of privacy invasion, a research group (Hawk, 2008), which managed to replicate Kerr and Stattin’s study (Stattin and Kerr, 2000), found that teenagers may consider active parental monitoring as a negative interference to privacy. They suggest that compared with gathering information via techniques, parents should explicitly express trust to their children and encourage them to share information. Leaving children full privacy may unsettle parents, since they cannot then stay updated and for them, it may be unbearable to imagine their children engaging in risky events. Children generally are not allowed to make important or difficult decisions without adults’ consent as they are assumed to be immature and inexperienced by parents and the surrounding. APA’s guidelines mentioned above partially manifests a needs-based framework of children’s rights, which stresses that children’s rights derive from their dependency on external protection and care. This framework presumes children are individuals with limited autonomy, requiring adults to tend to their needs as well as make decisions for them.
In contrary, a rather unique approach recently developed is based on autonomy, arguing that children should be granted rights in accordance with their evolving competence (Buss, 2004). Benjamin Shmueli and Ayelet Blecher-Prigat suggest children’s rights to privacy should be a combination right based on needs and autonomy. Shmueli and Blecher-Prigat note that the traditional understanding of privacy right centers on adult with full autonomy. Such a model excludes children from control over their privacy, since their level of autonomy does not meet the requirement. To challenge the conventional privacy right construct, they argue that children in different ages are not only entitled to parental care, but also allowed to control individual information, space and personal possessions and left in their discretion of handling personal issues, including revealing personal details online, establishing relationships with other individuals. When undergoing the decision making related to information disclosure and interpersonal interactions, children could strengthen their individuality and self-consciousness as well as creativity (Shmueli, 2010-2011).

Critics who oppose the autonomy-based framework of children right, argue that allowing children, particularly immature ones, to handle private issues might expose them to risks which could have been prevented by parental monitor. This concern does not reject the value of privacy to children, but poses a question that when a child should be let alone or a parent should refrain his control. In the children online privacy convention issued by UNICEF, it clearly states that children’s privacy should be respected in consistent with their advancing capacities. External assistance from parents, guardians and societies should be provided when children are not capable, while interference should be refrained as children mature (UNICEF, 2018).

Some parents might be anxious about the possibility that children would make themselves
an easy target by revealing their privacy online. This conventional assumption is based on a perception that children tend to act impulsively and are poor at decision making. Consequently, governments or public media (NSPC, 2019, Federal Bureau of Investigation, 2019, Council, 2019) suggest that parents take active control of children ICT privacy, such as deploying parental controls and checking browsing history. However, social research demonstrates that this one-for-all paternalistic approach might not be desirable. On the issue of different-aged children’s understanding of internet complexity, the research result shows that users who are between 5 and 10, lack capacities to identify cyber risks and are vulnerable to cyber bullying, so guardians’ instructions are necessary. But, as for teenage netizens, since rapid evolving mental development allows them to sense the adverse impact of irresponsible online activities, parental interference could be limited or even withdrawn (Yan, 2005). Regarding decision making, studies reveal that with their advancing mental developments, children could be well aware of consequences and make cautious decisions. Medical studies conducted on the topic of capability of teenagers’ medical decisions demonstrate that if they are correctly informed and advised, minors over 15 years old have attained competence to choose effective medical treatments (Mann, 1989).

Researches demonstrates that with their evolving cognitive and social developments, children are capable of dealing with privacy issues online. Parents who insist on carrying out invasive ICT-based monitoring regardless of children’s advancing competences, could undermine parent-child relationships. Mathiesen(Mathiesen, 2013) notes that trust is essential to intimate relationship, but once parental monitoring is discovered, children would have a strong feeling of being untrustworthy, impeding future conversations with parents. An episode
of science fiction TV series Black Mirror depicts an extreme case of parental control. In the show, an anxious mother takes her daughter to a clinic to install a microchip into her brain so the mother could access every aspect of her daughter’s life and determine what should be filtered by blocking her daughter’s vision. Being entirely deprived of privacy, the little girl eventually became an emotionless adult and distanced herself from her mother (Framke, 2017). This scenario might be exaggerated, but it does reveal what invasive parental monitoring might cost. It is understandable that parents would want to safeguard their children against harm whatever it takes, but this desire cannot justify that they take full control over children’s private domain. Shielding children from risky projects simultaneously decreases the possibility of personal enhancement, since activities involving a certain level of risks have been proved essential for a child to master social skills and become self-disciplined (Voce, 2008). The main adverse impact of invasive parental surveillance is creating mistrust, which further forms a vicious circle. When a child feels mistrusted, he will be reluctant to disclose personal information to his parents. The less a parent knows about his child, the more likely a parent would deploy monitor technique to gather his child’s recent information. Even for the sake of children’s best interests, parents should consider the extent and consequences of applying ICT-based technique to monitor minors.

A conundrum remaining in the issue of children ICT privacy is that since children have interests in privacy, on what grounds and to what level could a parent deploy ICT-based monitoring techniques? It would be discussed in the following chapter. To help address this conundrum, it would be useful to summarize what privacy should a child be in control regarding
his age. Lorrie Faith Cranor, a professor of Security and Privacy Technologies, initiated a project called Privacy Illustrated (Cranor, 2014), inviting people to paint what privacy means to them.

For children aged 9 to 12 (left), the majority of them describe privacy as their rooms and a few mention Internet, while for teenagers (right), their perception of privacy extends from physical space to social media and public surveillance.

To be more specific, the chart below demonstrates what is children’s online privacy.

---

2 Perception of privacy varies from person to person or from one generation to another. This summary attempts to offer a rough illustration, which may not be applicable to all children.


Chapter 3 Justification of ICT-based parental monitoring and Media literacy education

This chapter will first offer a framework to analyze the justification of parental monitoring with ICT. Then, it will suggest that children should be equipped with media literacy education, which could enable them to protect their privacy as well as instruct them to become responsible netizens.

3.1 Macnish’s theory and justifying ICT-based parental monitoring

Kevin Macnish proposes a theory, which draws on the just war to analyse the ethical justifiability of surveillance.

In Macnish’s theory, the justification of surveillance should be determined by two aspects, which are (1) justifying the decision to carry out surveillance and (2) justifying the means of surveillance (Macnish, 2014).
For the first examination, the conditions that could render the decision of surveillance justified are (1) just cause, (2) correct intention, (3) proper authority, (4) last resort, (5) formal declaration, (6) chance of success and (7) proportionality. Instead of being satisfied in a hierarchic order, these conditions should be combined when undertaking an ethical assessment. For instance, a justified intent for a government to deploying surveillance on the public should be to protect public security, while to discover political dissidents should be deemed immoral. The surveillance programme should be executed by proper parties, which are expected not to abuse the power. Last resort refers to a condition that public surveillance should be the last solution after other harmless approaches are deemed unfeasible. Formal declaration, as Macnish notes, indicates that people should be notified about the intent of the programme, while this practice could rule out the covert surveillance. As for chance of success and proportionality, Macnish suggests that the practice of monitoring can produce desirable result in accordance to the goal, while the damage of the practice must be minimized proportionally (Macnish, 2014).

The means of surveillance must be examined once the decision to carry out surveillance is made. Proportionality and discrimination are two factors requiring consideration. First, proportion of approaches of surveillance should be in accordance to the goal. For instance, if CCTV cameras can successfully gather information, then eavesdropping should not be applied as it is invasive. Second, discrimination suggests that if the goal of surveillance is to detect criminals, then only those who are suspicious should be targeted. But, it creates a problem that surveillance cannot distinguish criminals from the innocent until it gathers adequate evidence from large number of citizens, which may infringe the irrelevant people’s privacy (Macnish,
ICT-based parental monitoring is a form of surveillance, which could be subjected to Macnish’s framework. The critical issue is that children’s privacy may be at stake, when parents invasively monitor them with the assistance of ICT. Drawing on Macnish’s framework with slight modification, parental monitoring will be examined from two aspects, which are (1) justifying the decision of deploying monitoring and (2) justifying the means of monitoring. The decision of carrying out monitoring should be determined by (1) the intent of the practice, (2) necessity and (3) the acquisition of consent. As for examining the means of monitoring, proportionality should be of primary consideration.

The decision to carry out parental surveillance should be based on the intent of protecting children from harm or preventing them from engaging crimes. Children’s evolving competence should be considered when assessing harm. The rationale behind monitoring practice is when children are out of parents’ sight, knowing children’s whereabouts or activities allows parents to intervene in case of risky incidents. Parents place baby monitor devices, such as audio baby monitor or baby cameras in nursery room since they want to ensure that everything is going well in their young children’s rooms, while some medical experts have questioned the safety and effectiveness of those smart devices (Becker, 2017). In urban areas of China, parents of primary school students usually subscribe to a notification service jointly operated by schools and telecom providers, which sends text messages telling parents when children arrive at or leave schools (Baidu, 2019). Some parents are afraid their adolescent children cannot resist the temptation of alcohol and substance, or get involved with delinquencies, which renders parental monitoring necessary from their perspective (Stattin and Kerr, 2000). Harm and risk are
perception, which could be affected by age, gender, social experience, physical competence, social roles, etc. A 2m deep swimming pool can kill a child who is afraid of water, but it poses less threat to those who are adept at swimming. Students who are taught media literacy education may be less susceptible to manipulative advertisements, as a study finds that those who had participated in relevant courses are more skilled in analyzing advertisements and critical thinking than their counterparts in the control group (Hobbs, 2004). When deciding to carry out monitoring, it may be more desirable if the intent of parental monitoring can be based on parents’ and children’s perspectives. Knowing what children are able to deal with by themselves can help discover when a parent should intervene or let go. Assessing harm or risks without considering children’s competences could lead to overprotection, which may hinder children’s ability to assess risk and result in poor academic performance as well as cognitive defect (Ungar, 2009).

The intent of deploying monitoring answers the question why parents need to monitor children, while the analysis of necessity answers why the mean to meet parents’ intent has to be parental monitoring. Monitoring is a practice to observe an individual and gather information. For parents, monitoring provides them with the knowledge of their children’s whereabouts, activities, social relationships and website browsing history. More radically, with the cutting-edge wearable devices for children, parents can set geographical limit and get alerts when children leave the ‘safe zone’ (Frangoul, 2018). The necessity of deploying monitoring is connected to the willingness of children voluntarily disclosing information to their parents. For young children whose cognitive and verbal competences are limited, parental monitoring could serve as an auxiliary role to update children’s situation. Similarly, monitoring techniques can
help parents of children with special needs, such as specially designed GPS tracker to keep children on autism spectrum safe (Speaks, 2019). The necessity should be questioned as children mature. Compared with active monitoring, for teenagers, higher voluntary disclosure is related to lower delinquency rate. One possible explanation is that parents have created a reassuring environment to encourage information sharing, which strengthens parent-child relationships, resulting in preventing risky behavior (Stattin and Kerr, 2000). Some parents may argue that if my children refuse to talk to them, it is necessary for them to resort to deploying monitoring. Children’s rejection possibly derives from intense parent-child relationship, while insisting on carrying out monitoring could risk losing children’s trust, further deteriorating their willingness to disclosing information. Some other parents may claim parental monitoring is the most effective way to keep children from risk, so they have to adopt this practice. A study in the US finds that higher rate of health risk behaviors of teenagers is related to less parental monitoring, but the authors suggest parental monitoring be performed based on instructions and parents consider teenagers’ developing autonomy, instead of overprotecting (DiClemente et al., 2001). Besides preventing risk behaviors, a research examining the contributing factors of Chinese teenagers’ self-esteem reveals that parental monitoring, reasoning and autonomy granting are positive predictors of high self-esteem, while researchers note that harsh punishment or excessive parental control fails to reinforce self-esteem, contrasting with conventional Chinese tiger-parenting (Bush, 2002). Parents’ desire to acquire knowledge of their children’s location or activities could be met by monitoring or voluntary disclosure from children. The necessity of carrying out monitoring is affected by children’s competences and parent-child relationship.
Compared with good intent and necessity, the acquisition of consent may play a more critical role in maintaining mutual-trust family relationships. The consent given by children should be based on being well informed, instead of deception. Being well informed is the outcome of children receiving true information relevant to monitoring and children processing the information. A smart watch with GPS tracker sent by parents would receive great welcome from a five-year-old child, but teenagers might resent this device as they are clearly aware that real-time location data would be sent directly to their anxious parents. Parents’ reluctance to notify children of the practice of monitoring may be partially attributed to an assumption that once children are aware of monitoring, they may attempt to hide from monitoring, which could lead to dangerous situations, such as kidnapping or drowning. This assumption may be rooted in the conventional Chinese parenting. Chinese parenting style has been described as controlling and authoritarian (Chao, 1994). Through groups comparisons, Chinese mothers were found to have stronger preference for authoritative and authoritarian parenting style, which could be explained by their respect for Chinese values, emphasizing collectivism, norms abiding (Xu et al., 2005). In this sense, Chinese parents may assume that monitoring is to protect children’s interests, so children shall not resist that and parents have no need to ask for children’s consent, which could undermine children’s trust. In China, a study finds that both parent-child conversations and parental monitoring help parents gain knowledge of children’s activities, which has positive impact on child’s trust. The researches also note that invasive parental control depriving adolescent autonomy would boost teenagers’ insecurity, resulting in reluctance to further communication (Ying et al., 2015). Another study, which argues parental knowledge plays an important role in parent-child trust, reveals that compared with parental
monitoring, children’s active disclosure is a more reliable source of parental knowledge (Kerr et al., 1999). By asking children for their consent before carrying out monitoring, parents do not simply respect children’s privacy and autonomy, but, more importantly, state that they have faith in children, sincerely hoping to know more about children’s life, which may help strengthen familial trust.

Obtaining children’s consent requires parents to explain what monitoring is about to be carried out, which leads to the discussion of proportionality. Proportionality should be in consistent with the intent and the necessity, while sometimes they are intertwined. Potential risks brought by ICT, such as data leak, also need to be considered. The dominant principle should be that parents should choose the least invasive approach to gather children’s information. Busy working parents would be anxious about their children walking home alone, so a smart watch tracking children’s real-time location could help ease parents’ nerves. But it would be controversial and invasive if parents covertly install a spy application in children’s smartphones. A study intending to reveal children’s perception of parental control smartphone apps, demonstrates that children see parental control apps as a restrictive tool preventing them from accessing information and invading their privacy. What’s more, researchers find that if children are aware of the direct benefits, they are more inclined to using safety apps and have stronger willingness to share their feelings with their parents. Researchers note that the critical adverse impact of prevalent parental control is undermining parent-child trust (Ghosh et al., 2018). In case of safe Internet browsing, the following chart offers practical guidelines to parents of children in different age groups.
Another important issue worth considering is security and privacy risk. Blindly relying on ICT devices to gather children’s information may pose threat to children’s interests. In 2017, due to privacy safety concerns, Qihoo 360 shut down its video streaming service, which allowed parents to monitor children’s performance at school (Lee, 2017). In April 2019, Apple decided to remove several popular parental control app from App Store, reportedly for privacy concerns (Liptak, 2019). When deciding the mean to perform parental monitoring, parents should choose the least invasive and harmless approach to satisfy the goal of gaining knowledge of children.

ICT does serve as a useful tool for parents to track children to keep them safe, but it may raise ethical issues and bring risks to children’s privacy if ICT is invasively applied. Before deploying ICT-based monitoring, parents should examine the intent, the necessity as well as gain consent from children in advance. Proportionality of monitoring is also of equal importance.
3.2 Media literacy education

As mentioned in the previous chapters, the number of underage Internet users has rapidly grown in China, which indicates that children are more likely to come across privacy issues. Deploying parental surveillance could be helpful in some situations, but it is also critical to prepare children to safeguard themselves as they have interests in their privacy. Media literacy education could be appropriate to prepare children for future ICT privacy issues.

Media literacy education aims at teaching students to understand and interact with media. By undertaking media literacy training, young people would be able to interpret the media contexts and make informed judgments with critical thinking (Buckingham, 2013). The emergence of ICT has posed great challenge to traditional media education, which simply focuses on printed media, like books and TV programmes or films. ICT has extended the form of media to a new dimension, where audiences are enabled to create and spread contexts to other audiences by updating posts on social media such as Facebook and Instagram. Given this radical change of media landscape and audience-media relationship, the goal of media literacy training should center practical skills to assist individuals to acquire literacy. A set of skills relevant to attaining literacy include four aspects, which are access, analysis, evaluation, and content creation (LIVINGSTONE, 2004). According to UNESCO, one main benefit provided by media literacy education is by learning media literacy, young citizens can become independent, critical and reflective thinkers. The following chart illustrates the competency related to ICT (UNESCO, 2013):
In China, media literacy is taught in several ways. For example, the curriculum can be designed by a college and delivered by a primary or secondary school. In some cases, media literacy education is conceived and executed by voluntary teachers. At the state level, some organizations, such as China Children’s Press and Publication Group (CCPPG), have attempted to introduce relevant courses to primary school students (Cheung and Xu, 2016). A report suggests that to guarantee success of media literacy education, the curriculum should be better
integrated into the school system and collaboration with NGO or education departments is of great help (Mihailidis, 2009). To support children to receive media literacy training, it requires joint efforts from families, schools, local communities, governments, mass media and technology companies. For instance, local governments could fund teacher training programmes, which could enable teachers to deliver systematic courses. Media and technology companies could provide free materials and tools to students, so they can practice analytical skills. At home, parents can instruct children to choose appropriate media context (Hobbs, 2010).

Chapter 4: Conclusion

China has witnessed rapid development in Information and communications technology, with dramatically growing number of underage Internet users. With the aid of ICT, parents can use wearable devices, smartphones apps or cameras to monitor children, which may raise ethical issues of invading children’s privacy. Compared with children online privacy protection in western countries, such as COPPA and GDPR, China is lagging behind.

Conventionally, children are seen as individuals with limited autonomy and competency. Therefore, it appears to be dangerous to allow children to be in control of their privacy, which renders parental monitoring necessary. As this thesis argues, children do have interests in their privacy, both online and offline. According to the advancing cognitive and social development, children become more capable of dealing their privacy issues.

As parental monitoring may infringe children’s privacy, it is necessary to examine the
justification of the monitoring practice. Drawing on Macnish’s theory, the intent and necessity of monitoring should be discussed. Children should be informed of the upcoming monitoring and their consent should be acquired in advance. When deciding the mean to carry out monitoring, the least invasive and the most necessary approaches should be given prior consideration. Apart from parental monitoring, states, schools and families should educate children on media literacy, so children can become a responsible ICT users and protect themselves from online privacy infringement and cyber bullying.
References

[Accessed 2019].


BAIDU. 2019. 家校通 [Online]. Available: https://baike.baidu.com/item/%E5%AE%B6%E6%A0%A1%E9%80%9A


CAC 2016. 未成年人网络保护条例(送审稿).


CONTRIBUTORS, W. 2019b. *Information and communications technology* [Online].


KELLY, M. 2013. These 5 countries were ranked best for privacy (infographic) [Online]. Available: https://venturebeat.com/2013/10/13/countries-privacy/ [Accessed 22.April 2019].


SAC 2018. Personal information security specification. In: SAC (ed.).


UNGAR, M. 2009. Overprotective Parenting: Helping Parents Provide Children the


